The Value of Email DLP

Identifying and Minimizing Your Organization's Greatest Risk

By ZixCorp
www.zixcorp.com

CLICKING 'SEND' IS ALMOST TOO EASY.

We've all had those moments when we wince slightly for sending an email too soon. You forwarded the joke to your CEO Bill instead of your old friend Bill. You forgot to insert an attachment to the message – the only reason for your email in the first place. Perhaps you sent a "sorry" reply or just crossed your fingers that the email was lost among the hundreds received a day. As painful as those moments are, the result can be far worse than slight embarrassment.

Protected health information, financial data and other sensitive corporate information are exchanged regularly, as companies communicate throughout the day to patients, customers, business associates and vendors. Email encryption can be used to protect sensitive data in transmission, but what if email shouldn't be sent in the first place?

Even if you exhaust your employee training options, mistakes are going to happen. Data loss prevention (DLP) can identify and minimize that risk. More importantly, it can protect your company from the associated costs – fraud protection, regulatory fines and potential civil lawsuits.

Mistakes are going to happen. Data loss prevention (DLP) can identify and minimize that risk and protect your company from the associated costs.

EMAIL DLP USE CASES

Once an email leaves your secure network by mistake, there are few options to remedy the issue.

If luck has it, your sender realized his or her error, and your organization can address it immediately – with a recall tool or a hopeful "please destroy" follow-up message. If not, perhaps the recipient is kind enough to notify your organization and chooses not to misuse the sensitive information. However, with the sheer number of emails exchanged per day, odds are that you may not know for months (or ever) when an email is sent in error. And we all know it can happen in several different ways.

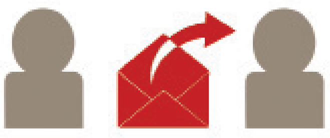
Right Email, Wrong Recipient

Auto-populate can be a dangerous convenience. With a single key stroke, you can add an inappropriate recipient to an email with credit card information, social security numbers or protected health information. Email DLP removes that risk by identifying content in the subject line, message and attachment that should not be sent to specific recipients. Whether a policy determines the recipient should have a certain domain or shouldn't have a Webmail address, DLP can prevent that message from ever leaving your organization.

Real World Report

An employee with The Regional Medical Center of Memphis mistakenly sent 1,200 patient records to the wrong outside organization. The breach went undiscovered until an internal audit recognized the error.

Right Recipient, Wrong File



Many employees need access to a variety of sensitive data to conduct their day-to-day responsibilities. Often they appropriately send sensitive data outside the company, but within easy reach, it's simple to attach the wrong document to an unrelated email. Email DLP can prevent that attachment from leaving your organization by identifying sensitive data contained in the email and quarantining it for review. Upon automatic notification, the sender has the opportunity to correct any mistakes, including the attachment of a wrong file.

Real World Report

An employee with California-based Stanford Federal Credit Union inadvertently attached personal information for 18,000 members in an email to another member. The breach was recognized immediately but still required that affected members be notified.

EMAIL DLP USE CASES (CONT'D.)

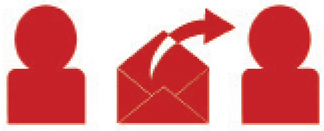
Wrong Sender

Employees are often recognized as the most valuable asset of an organization. While you trust them to use sensitive data to conduct business, not every employee needs to exchange it outside the company to get their job done. Whether you want to limit the exchange of sensitive data by department, role or individual, email DLP can provide that control.

Real World Report

Confidential information of more than 10,000 patients of Dent Neurologic Institute was inadvertently sent by a clerk to more than 200 patients. Without any other methods to correct the error, the recipients were simply asked to delete the message.

Intentional Misuse



Most use cases for email DLP will involve protecting the company from the mistakes of good-hearted employees, but there are rare cases where an employee deliberately sends email for inappropriate gain. A customer list, intellectual property for a new product or personal information on a patient or customer – no matter the data, email DLP is a valuable component for protecting your company.

Real World Report

For years, a vice president and computer programmer with Goldman Sachs was emailing confidential files to his personal email account. After leaving Goldman Sachs for a new position, his acts were discovered when he transferred a substantial amount of proprietary data outside the company on his last day of employment. Arrested and convicted for theft of trade secrets and interstate transportation of stolen property, the former employee received 97 months in prison and a $12,500 fine.

THE ADVANTAGES OF SINGLE APPLICATION DLP

To prevent sensitive email from leaving your enterprise in an unauthorized manner, your organization can implement a full DLP solution or single-application DLP. Extremely comprehensive tools, full DLP solutions can analyze all channels of risk and prevent sensitive data from leaving your enterprise in any manner. They also establish one standard for rules, policies and procedures across the whole organization and through a single interface.

In theory, full DLP offers a valuable tool for data protection. However, in practice, organizations have experienced an overwhelming challenge that exceeds budgets and timelines. According to Forrester Research Report *Rethinking DLP*, "Despite 89% of security stakeholders citing data security as their No. 1 challenge, our research indicates that only about one-quarter of enterprise customers have implemented DLP technologies. Additionally, customer feedback indicates that about half of the companies that have implemented DLP consider those deployments to have failed at some level." The report continues with, "Many deployments take longer than expected and require more resources than anticipated and budgeted for. These changing conditions have left DLP half done in many organizations, thereby creating a level of frustration for project owners."

In contrast, single-application DLP can effectively manage the channels that pose the greatest risks. By focusing on one channel, single-application DLP is not only cost-effective but also quick to deploy. Once the greatest risk is addressed, then your organization can analyze other channels and determine any additional needs, making the roll-out of DLP more manageable and costs more predictable.

Single-application DLP can effectively manage the channels that pose the greatest risks, making the roll-out of DLP more manageable and costs more predictable.

Real World Report: What do you consider Warp Speed? A recent case study highlighted the successful launch of a full DLP solution. In promoting the case study, the solution provider claimed the deployment occurred in "Warp Speed," taking only 5 months to complete with the assistance of 375 engineers.

THE VALUE OF ZIXQUARANTINE

ZixQuarantine offers an email-specific DLP solution for enhanced data protection and at a low, predictable cost per user per year.. It can be deployed in hours instead of months, and it requires minimal effort from your team without any additional resources or consultants. These high-level business benefits complement the superior technology that enables organizations to build from our company's decade of security experience and grow with the solution as their needs change.

PROVEN POLICIES

Our company spent more than 10 years earning its reputation as the industry leader in email encryption. Ease of use is our key differentiator, and a component of that achievement is proven policy filters that identify sensitive information. Through a decade of experience and customer feedback, we refined these policies to meet strict obligations – often outlined by regulatory requirements – and gain the trust of the nation's most influential organizations, including:

- All federal financial regulators, including FFIEC
- Five divisions of the U.S. Treasury
- The U.S. Securities and Exchange Commission
- More than 20 state regulators
- One in every four U.S. banks
- More than 30 Blue Cross Blue Shield organizations
- One in every five U.S. hospitals

In developing ZixQuarantine, we leveraged these policies with quarantine policies to offer industry-leading, sophisticated scanning capabilities. Our proven policies allow organizations to identify sensitive information in email (without the need for hundreds of consultants) and build on their strength with custom policies to address unique organizational needs.

	ZIXQUARANTINE
Low, predictable cost	✓
Deployed in hours, not months	✓
Requires minimal effort from your team	✓
Easy to use	✓

EDUCATION AND TRAINING THROUGH A CONVENIENT USER EXPERIENCE

When a policy is triggered, the email is sent to ZixQuarantine. Through an email notification, employees can easily access the quarantined email, view what part of the email was identified as sensitive and gain a better understanding of what policy was triggered to quarantine the message. By interacting with the email and taking these extra steps, employees become more aware of corporate policies and more alert to the sensitivity of valuable information. It supports additional education and training that may already be in place and reinforces a workplace culture that values patient or customer privacy and proprietary corporate information.

ZixQuarantine supports additional education and training that may already be in place and reinforces a workplace culture that values patient or customer privacy and proprietary corporate information.

FLEXIBLE DEPLOYMENT OPTIONS

In evaluating the need for an email DLP solution, some organizations may immediately recognize the risk whereas others may want validation. Similarly, with a solution in place, some organizations may immediately cease all outbound email that violates policies whereas others may gradually restrict communication as employees interact with the new email DLP capabilities. Regardless of your organization's approach, Zix offers two versions to meet your unique needs.

ZixQuarantine offers all scanning and quarantining controls for organizations that face heavy regulatory burdens or corporate security concerns and need to promptly address breach risks. For companies that can take a gradual approach, ZixInsight is a simplified version that can be used to identify the data risks in email and understand how quarantining messages will impact your employees, recipients and overall business workflow.

EASY ADMINISTRATIVE CONTROLS

Beyond the convenience of deployment, administrators can leverage the intuitive interface to manage ZixQuarantine or ZixInsight. In monitoring messages with sensitive information, individual or multiple quarantined emails can be released or deleted with one click. Message review can also be the responsibility of one or more administrators or distributed to business units. For visibility into overall trends, administrators can use flexible searching and filtering options or rely on reports to summarize the organization's activities.

KEEP THE EASE OF CLICKING 'SEND' WITHOUT THE RISK

Mistakes happen, and given the frequency that we click the 'Send' button, it's no surprise that they happen often in email. Whether it's adding the wrong recipient, attaching the wrong file or trusting the wrong person, sensitive data is inappropriately leaving your organization in email.

Let Zix help you understand the full extent of the challenge and minimize your greatest risk.

Zix Corporation . 2711 N. Haskell Avenue . Suite 2300, LB 36 . Dallas, TX 75204
Phone 866 257 4949 . sales@zixcorp.com . www.zixcorp.com